UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/737,627	12/15/2000	Alastair John Angwin	GB919990123US1	7824

25259 7590 05/21/2004

IBM CORPORATION
3039 CORNWALLIS RD.
DEPT. T81 / B503, PO BOX 12195
REASEARCH TRIANGLE PARK, NC 27709

EXAMINER	
PARTHASARATHY, PRAMILA	
ART UNIT	**PAPER NUMBER**
2136	4

DATE MAILED: 05/21/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/737,627	ANGWIN ET AL.	
	Examiner	Art Unit	
	Pramila Parthasarathy	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *23 May 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-26* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-26* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date #2.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to the communication filed on 05/23/2001. Claims 1 – 26 were received for consideration. NO preliminary amendments to the specification were filed. Claims 1 – 26 are currently being considered.

Specification

Claim 18 is objected to because of the following informalities: "and a one-way has function" should be replaced with "and a one-way hash function.

Appropriate correction is required.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1- 20, and 23 - 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Trieger (U.S. Patent No.: 6,226,750) in view of Anderson (U.S. Patent No.: 5,751,812).

Regarding Claim 1, Trieger teaches and describes a method of controlling a plurality of separate electronic communications between said first and second parties (Fig. 1 – 4 and Column 6 line 30 – Column 10 line 26), said method comprising the steps of:

(a) initially securely exchanging a seed value between said first and second parities (Column 7 line 48 – Column 8 line 30 and Column 10 lines 42 – 56);

(b) exchanging a mathematical advance function between said parties (Column 7 line 48 – Column 8 line 30 and Column 10 lines 42 – 56); and

(c) exchanging a one-way hash function between said parties (Column 7 line 48 – Column 8 line 30 and Column 10 lines 42 – 56);

said method further comprising, prior to each separate communication, the step of:

(d) applying said advance function to the seed value to create a new seed value at each of said parities (Column 11 lines 44 – 66 and Column 12 lines 18 – 47);

(e) applying said hash function to said new seed value to create a said security code at each of said parties (Column 11 lines 44 – 66 and Column 12 lines 18 – 47);

(f) communicating said security code generated at said first party to said second party (Column 11 lines 44 – 66 and Column 12 lines 18 – 47);

(g) comparing said communicated security code with said security code generated at said second party (Column 8 line 62 – Column 9 line 32); and

(h) if said security codes are the same at both parties, permitting the respective communication to take place between said first and second parties (Column 8 line 62 – Column 9 line 60).

Trieger does not explicitly disclose exchanging a seed value, a mathematical advance function and exchanging a one-way hash function. However, Anderson discloses a method and apparatus for re-initialization function which may be implemented without the need for additional information from the user, the steps comprising:

(a) initially securely exchanging a seed value between said first and second parities (Anderson Column 1 line 60 – Column 2 line 5);

(b) exchanging a mathematical advance function between said parties (Anderson Column 1 line 60 – Column 2 line 5); and

(c) exchanging a one-way hash function between said parties (Anderson Column 1 line 60 – Column 2 line 5);

said method further comprising, prior to each separate communication, the step of:

(d) applying said advance function to the seed value to create a new seed value at each of said parities (Anderson Column 6 lines 13 – 33);

(e) applying said hash function to said new seed value to create a said security code at each of said parties (Anderson Column 6 lines 13 – 33);

(f) communicating said security code generated at said first party to said second party (Anderson Column 6 lines 13 – 33);

(g) comparing said communicated security code with said security code generated at said second party (Anderson Column 6 lines 13 – 44); and

(h) if said security codes are the same at both parties, permitting the respective communication to take place between said first and second parties (Anderson Column 6 lines 13 – 50).

Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of communication between first party and second party to exchange a seed value, a mathematical advance function and one-way hash function as taught by Anderson and comparing security code with the generated security code to permit the respective communication to take place as taught by Trieger to provide automatic re-initialization. The motivation would have been to provide improved secure systems in terms of re-initialization security and convenience.

Regarding Claim 7, Trieger teaches and describes a system comprising means of controlling a plurality of separate electronic communications between said first and second parties, by exchange of security codes between said parties (Fig. 1 – 4 and Column 6 line 30 – Column 10 line 26); wherein said means for controlling includes:

means for initially securely exchanging a seed value between said first and second parities (Column 7 line 48 – Column 8 line 30 and Column 10 lines 42 – 56);

means for exchanging a mathematical advance function between said parties (Column 7 line 48 – Column 8 line 30 and Column 10 lines 42 – 56); and

means for exchanging a one-way hash function between said parties (Column 7 line 48 – Column 8 line 30 and Column 10 lines 42 – 56);

means for applying said advance function to the seed value to create a new seed value at each of said parities prior to each separate communication (Column 11 lines 44 – 66 and Column 12 lines 18 – 47);

means for applying said hash function to said new seed value to create a said security code at each of said parties (Column 11 lines 44 – 66 and Column 12 lines 18 – 47);

means for communicating said security code generated at said first party to said second party (Column 11 lines 44 – 66 and Column 12 lines 18 – 47);

means for comparing said communicated security code with said security code generated at said second party (Column 8 line 62 – Column 9 line 32); and

means responsive to said security codes being the same at both parties to permit the respective communication to take place between said first and second parties (Column 8 line 62 – Column 9 line 60).

Trieger does not explicitly disclose exchanging a seed value, a mathematical advance function and exchanging a one-way hash function. However, Anderson discloses a method and apparatus for re-initialization function which may be implemented without the need for additional information from the user, the steps comprising:

means for initially securely exchanging a seed value between said first and second parties (Anderson Column 1 line 60 – Column 2 line 5);

means for exchanging a mathematical advance function between said parties (Anderson Column 1 line 60 – Column 2 line 5); and

means for exchanging a one-way hash function between said parties (Anderson Column 1 line 60 – Column 2 line 5);

means for applying said advance function to the seed value to create a new seed value at each of said parities (Anderson Column 6 lines 13 – 33);

means for applying said hash function to said new seed value to create a said security code at each of said parties (Anderson Column 6 lines 13 – 33);

means for communicating said security code generated at said first party to said second party (Anderson Column 6 lines 13 – 33);

means for comparing said communicated security code with said security code generated at said second party (Anderson Column 6 lines 13 – 44); and

means for responsive to said security codes being the same at both parties to permit the respective communication to take place between said first and second parties (Anderson Column 6 lines 13 – 50).

Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of communication between first party and second party to exchange a seed value, a mathematical advance function and one-way hash function as taught by Anderson and comparing security code with the generated security code to permit the respective communication to take place as taught

by Trieger to provide automatic re-initialization. The motivation would have been to provide improved secure systems in terms of re-initialization security and convenience.

Regarding Claim 12, Trieger teaches and describes a computer program for use in an electronic communication system for providing communication between at least first party and a second party, said computer program comprising instructions carry out a method of controlling a plurality of separate electronic communications between said first and second parties (Fig. 1 – 4 and Column 6 line 30 – Column 10 line 26), comprising the steps of:

(a) initially securely exchanging a seed value between said first and second parities (Column 7 line 48 – Column 8 line 30 and Column 10 lines 42 – 56);

(b) exchanging a mathematical advance function between said parties (Column 7 line 48 – Column 8 line 30 and Column 10 lines 42 – 56); and

(c) exchanging a one-way hash function between said parties (Column 7 line 48 – Column 8 line 30 and Column 10 lines 42 – 56);

said method further comprising, prior to each separate communication, the step of:

(d) applying said advance function to the seed value to create a new seed value at each of said parities (Column 11 lines 44 – 66 and Column 12 lines 18 – 47);

(e) applying said hash function to said new seed value to create a said security code at each of said parties (Column 11 lines 44 – 66 and Column 12 lines 18 – 47);

(f) communicating said security code generated at said first party to said second party (Column 11 lines 44 – 66 and Column 12 lines 18 – 47);

(g) comparing said communicated security code with said security code generated at said second party (Column 8 line 62 – Column 9 line 32); and

(h) if said security codes are the same at both parties, permitting the respective communication to take place between said first and second parties (Column 8 line 62 – Column 9 line 60).

Trieger does not explicitly disclose exchanging a seed value, a mathematical advance function and exchanging a one-way hash function. However, Anderson discloses a method and apparatus for re-initialization function which may be implemented without the need for additional information from the user, the steps comprising:

(a) initially securely exchanging a seed value between said first and second parities (Anderson Column 1 line 60 – Column 2 line 5);

(b) exchanging a mathematical advance function between said parties (Anderson Column 1 line 60 – Column 2 line 5); and

(c) exchanging a one-way hash function between said parties (Anderson Column 1 line 60 – Column 2 line 5);

said method further comprising, prior to each separate communication, the step of:

(d) applying said advance function to the seed value to create a new seed value at each of said parities (Anderson Column 6 lines 13 – 33);

(e) applying said hash function to said new seed value to create a said security code at each of said parties (Anderson Column 6 lines 13 – 33);

(f) communicating said security code generated at said first party to said second party (Anderson Column 6 lines 13 – 33);

(g) comparing said communicated security code with said security code generated at said second party (Anderson Column 6 lines 13 – 44); and

(h) if said security codes are the same at both parties, permitting the respective communication to take place between said first and second parties (Anderson Column 6 lines 13 – 50).

Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of communication between first party and second party to exchange a seed value, a mathematical advance function and one-way hash function as taught by Anderson and comparing security code with the generated security code to permit the respective communication to take place as taught by Trieger to provide automatic re-initialization. The motivation would have been to provide improved secure systems in terms of re-initialization security and convenience.

Regarding Claim 18, Trieger teaches and describes a client computer connectable for secure communication with a server computer (Fig. 1 – 4 and Column 6 line 30 – Column 10 line 26), said client computer comprising:

means for receiving from said server computer a seed value, a mathematical advance function and a one-way hash function (Column 7 line 48 – Column 8 line 30 and Column 10 lines 42 – 56);

means for said hash function to said new seed value to create a security code (Column 11 lines 44 – 66 and Column 12 lines 18 – 47); and

means for communicating said security code to said server computer (Column 11 lines 44 – 66 and Column 12 lines 18 – 47);

whereby said server computer permits secure communication with said client computer is security code correspondingly calculated by said server is identical to said security codes communicated by said client computer (Column 8 line 62 – Column 9 line 60).

Trieger does not explicitly disclose exchanging a seed value, a mathematical advance function and exchanging a one-way hash function. However, Anderson discloses a method and apparatus for re-initialization function which may be implemented without the need for additional information from the user, the steps comprising:

means for receiving from said server computer a seed value, a mathematical advance function and a one-way hash function (Anderson Column 1 line 60 – Column 2 line 5);

means for said hash function to said new seed value to create a security code (Anderson Column 6 lines 13 – 33); and

means for communicating said security code to said server computer (Anderson Column 6 lines 13 - 33);

whereby said server computer permits secure communication with said client computer is security code correspondingly calculated by said server is identical to said security codes communicated by said client computer (Anderson Column 6 lines 13 – 50).

Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of communication between first party and second party to exchange a seed value, a mathematical advance function and one-way hash function as taught by Anderson and comparing security code with the generated security code to permit the respective communication to take place as taught by Trieger to provide automatic re-initialization. The motivation would have been to provide improved secure systems in terms of re-initialization security and convenience.

Regarding Claim 24, Trieger teaches and describes a server computer connectable for secure communication with one or more client computers (Fig. 1 – 4 and Column 6 line 30 – Column 10 line 26), said server computer comprising means for providing to said client computer a seed value, a mathematical advance function and a one-way hash function (Column 7 line 48 – Column 8 line 30 and Column 10 lines 42 – 56);

means for applying said advance function to said seed value to create a new seed value at each of said parities prior to each separate communication (Column 11 lines 44 – 66 and Column 12 lines 18 – 47);

means for applying said hash function to said new seed value to create a security code (Column 11 lines 44 – 66 and Column 12 lines 18 – 47);

means for receiving a correspondingly calculated security code from said client compute (Column 11 lines 44 – 66 and Column 12 lines 18 – 47);

means for comparing said communicated security codes (Column 8 line 62 – Column 9 line 32); and

means responsive to said security codes being the same to enable secure communication to take place with said client computer (Column 8 line 62 – Column 9 line 60).

Trieger does not explicitly disclose exchanging a seed value, a mathematical advance function and exchanging a one-way hash function. However, Anderson discloses a method and apparatus for re-initialization function which may be implemented without the need for additional information from the user, the steps comprising:

means for providing to said client computer a seed value, a mathematical advance function and a one-way hash function (Anderson Column 6 lines 13 - 33);

means for applying said advance function to said seed value to create a new seed value at each of said parities prior to each separate communication (Anderson Column 6 lines 13 - 33);

means for applying said hash function to said new seed value to create a security code (Anderson Column 6 lines 13 - 33);

means for receiving a correspondingly calculated security code from said client compute (Anderson Column 6 lines 13 - 33);

means for comparing said communicated security codes (Anderson Column 6 lines 13 - 44); and

means responsive to said security codes being the same to enable secure communication to take place with said client computer (Anderson Column 6 lines 13 – 50).

Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of communication between first party and second party to exchange a seed value, a mathematical advance function and one-way hash function as taught by Anderson and comparing security code with the generated security code to permit the respective communication to take place as taught by Trieger to provide automatic re-initialization. The motivation would have been to provide improved secure systems in terms of re-initialization security and convenience.

Claim 2 is rejected as applied above in rejecting claim 1. Furthermore, Triegar teaches and describes a method of controlling a plurality of separate electronic communications between said first and second parties (Fig. 1 – 4 and Column 6 line 30 – Column 10 line 26), wherein said separate communications each follow a disconnection of said first and second parties, said steps (a) to (c) preceding such

disconnection, said method including the further step of physically re-establishing said connection between said parties prior to said steps (d) to (g) (Column 3 lines 38 – 65; Column 8 line 62 – Column 9 line 32; Column 10 lines 42 – 56; Column 11 lines 44 –66; and Column 12 lines 18 – 47).

Claim 3 is rejected as applied above in rejecting claim 1. Furthermore, Trieger teaches and describes a method of controlling a plurality of separate electronic communications between said first and second parties (Fig. 1 – 4 and Column 6 line 30 – Column 10 line 26), wherein said advance function is non-recursive (Anderson Column 5 lines 35 – 50).

Claim 5 is rejected as applied above in rejecting claim 1. Furthermore, Trieger teaches and describes a method of controlling a plurality of separate electronic communications between said first and second parties (Fig. 1 – 4 and Column 6 line 30 – Column 10 line 26), wherein said advance function is an arithmetic function (Anderson Column 5 lines 35 – 50 and Column 6 lines 13 – 33).

Claim 6 is rejected as applied above in rejecting claim 1. Furthermore, Trieger teaches and describes a method of controlling a plurality of separate electronic communications between said first and second parties (Fig. 1 – 4 and Column 6 line 30 – Column 10 line 26), in which, if said security code is the same, after comparing step

(g), comprises further, steps, prior to permitting resumption of communication between said first and second parties, of:

applying the advance function to said new seed value at each of said parties to create a further new seed value (Column 11 lines 44 – 66 and Column 12 lines 18 – 47; Anderson Column 6 lines 13 – 33);

applying the hash function to said further new seed value to create a further security code at each of said parties (Column 11 lines 44 – 66 and Column 12 lines 18 – 47; Anderson Column 6 lines 13 – 33);

communicating said further security code generated at said second party to said first party (Column 11 lines 44 – 66 and Column 12 lines 18 – 47; Anderson Column 6 lines 13 – 33);

comparing said further security codes received at said first party with the further security code generated at said first party (Column 8 line 62 – Column 9 line 32 and Anderson Column 6 lines 13 – 44); and

if said further security code is also the same at both nodes, permitting said communication between said first and second parties to take place (Column 8 line 62 – Column 9 line 60 and Anderson Column 6 lines 13 – 50).

Claim 8 is rejected as applied above in rejecting claim 7. Furthermore, Trieger teaches and describes a system comprising means of controlling a plurality of separate electronic communications between said first and second parties, by exchange of security codes between said parties (Fig. 1 – 4 and Column 6 line 30 – Column 10 line

26); wherein said separate communication each follow a disconnection of said first and second parties, said system including means for physically re-establishing said connection between said parties (Column 3 lines 38 – 65).

Claim 9 is rejected as applied above in rejecting claim 7. Furthermore, Trieger teaches and describes a system comprising means of controlling a plurality of separate electronic communications between said first and second parties, by exchange of security codes between said parties (Fig. 1 – 4 and Column 6 line 30 – Column 10 line 26). wherein said advance function is non-recursive (Anderson Column 5 lines 35 – 50).

Claim 11 is rejected as applied above in rejecting claim 7. Furthermore, Trieger teaches and describes a system comprising means of controlling a plurality of separate electronic communications between said first and second parties, by exchange of security codes between said parties (Fig. 1 – 4 and Column 6 line 30 – Column 10 line 26), including said means for exchanging said advance function and said hash function securely (Anderson Column 6 lines 33).

Claim 13 is rejected as applied above in rejecting claim 12. Furthermore, Trieger teaches and describes a computer program for use in an electronic communication system for providing communication between at least first party and a second party, said computer program comprising instructions carry out a method of controlling a plurality of separate electronic communications between said first and second parties

(Fig. 1 – 4 and Column 6 line 30 – Column 10 line 26), wherein said separate communications each follow a disconnection of said first and second parties, said steps (a) to (c) preceding such disconnection, said method including the further step of physically re-establishing said connection between said parties prior to said steps (d) to (g) (Column 3 lines 38 – 65; Column 8 line 62 – Column 9 line 32; Column 10 lines 42 – 56; Column 11 lines 44 –66; and Column 12 lines 18 – 47).

Claim 14 is rejected as applied above in rejecting claim 12. Furthermore, Trieger teaches and describes a computer program for use in an electronic communication system for providing communication between at least first party and a second party, said computer program comprising instructions carry out a method of controlling a plurality of separate electronic communications between said first and second parties (Fig. 1 – 4 and Column 6 line 30 – Column 10 line 26), wherein said advance function is non-recursive (Anderson Column 5 lines 35 – 50).

Claim 16 is rejected as applied above in rejecting claim 12. Furthermore, Trieger teaches and describes a computer program for use in an electronic communication system for providing communication between at least first party and a second party, said computer program comprising instructions carry out a method of controlling a plurality of separate electronic communications between said first and second parties (Fig. 1 – 4 and Column 6 line 30 – Column 10 line 26), wherein said advance function and said hash function are also exchanged securely (Anderson Column 6 lines 3 – 33).

Claim 17 is rejected as applied above in rejecting claim 12. Furthermore, Trieger teaches and describes a computer program for use in an electronic communication system for providing communication between at least first party and a second party, said computer program comprising instructions carry out a method of controlling a plurality of separate electronic communications between said first and second parties (Fig. 1 – 4 and Column 6 line 30 – Column 10 line 26), in which, if said security code is the same, after comparing step (g), comprises further, steps, prior to permitting resumption of communication between said first and second parties, of:

applying the advance function to said new seed value at each of said parties to create a further new seed value (Column 11 lines 44 – 66 and Column 12 lines 18 – 47; Anderson Column 6 lines 13 – 33);

applying the hash function to said further new seed value to create a further security code at each of said parties (Column 11 lines 44 – 66 and Column 12 lines 18 – 47; Anderson Column 6 lines 13 – 33);

communicating said further security code generated at said second party to said first party (Column 11 lines 44 – 66 and Column 12 lines 18 – 47; Anderson Column 6 lines 13 – 33);

comparing said further security codes received at said first party with the further security code generated at said first party (Column 8 line 62 and Column 9 line 32; Anderson Column 6 lines 13 – 44); and

if said further security codes are also the same at both parties, permitting said communication between said first and second parties to take place (Column 8 line 62 – Column 9 line 60; Anderson Column 6 lines 13 – 50).

Claim 19 is rejected as applied above in rejecting claim 18. Furthermore, Trieger teaches and describes a client computer connectable for secure communication with a server computer (Fig. 1 – 4 and Column 6 line 30 – Column 10 line 26), wherein said advance function is non-recursive (Anderson Column 5 lines 35 – 50).

Claim 25 is rejected as applied above in rejecting claim 24. Furthermore, Trieger teaches and describes a server computer connectable for secure communication with one or more client computers (Fig. 1 – 4 and Column 6 line 30 – Column 10 line 26), said server computer comprising means for providing to said client computer a seed value, a mathematical advance function and a one-way hash function (Column 7 line 48 – Column 8 line 30 and Column 10 lines 42 – 56); wherein said advance function is non-recursive (Anderson Column 5 lines 35 – 50).

Claim 4 is rejected as applied above in rejecting claim 3. Furthermore, Trieger teaches and describes a method of controlling a plurality of separate electronic communications between said first and second parties (Fig. 1 – 4 and Column 6 line 30 – Column 10 line 26), wherein said advance function is an arithmetic function (Anderson Column 5 lines 35 – 50 and Column 6 lines 13 – 33).

Claim 10 is rejected as applied above in rejecting claim 9. Furthermore, Trieger teaches and describes a system comprising means of controlling a plurality of separate electronic communications between said first and second parties, by exchange of security codes between said parties (Fig. 1 – 4 and Column 6 line 30 – Column 10 line 26); wherein said advance function is an arithmetic function (Anderson Column 5 lines 35 – 50 and Column 6 lines 13 – 33).

Claim 15 is rejected as applied above in rejecting claim 14. Furthermore, Trieger teaches and describes a computer program for use in an electronic communication system for providing communication between at least first party and a second party, said computer program comprising instructions carry out a method of controlling a plurality of separate electronic communications between said first and second parties (Fig. 1 – 4 and Column 6 line 30 – Column 10 line 26), wherein said advance function is an arithmetic function (Anderson Column 5 lines 35 – 50 and Column 6 lines 13 – 33).

Claim 20 is rejected as applied above in rejecting claim 19. Furthermore, Trieger teaches and describes a client computer connectable for secure communication with a server computer (Fig. 1 – 4 and Column 6 line 30 – Column 10 line 26), wherein said advance function is an arithmetic function (Anderson Column 5 lines 35 – 50 and Column 6 lines 13 – 33).

Claim 26 is rejected as applied above in rejecting claim 25. Furthermore, Trieger teaches and describes a server computer connectable for secure communication with one or more client computers (Fig. 1 – 4 and Column 6 line 30 – Column 10 line 26), said server computer comprising means for providing to said client computer a seed value, a mathematical advance function and a one-way hash function (Column 7 line 48 – Column 8 line 30 and Column 10 lines 42 – 56); wherein said advance function is an arithmetic function (Anderson Column 5 lines 35 – 50 and Column 6 lines 13 – 33).

Claims 21 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Trieger (U.S. Patent No.: 6,226,750) in view of Anderson (U.S. Patent No.: 5,751,812) further in view of Owens et al. (U.S. Patent No.: 6, 338,140).

Claim 21 is rejected as applied above in rejecting claim 18. Furthermore, Trieger teaches and describes a client computer connectable for secure communication with a server computer (Fig. 1 – 4 and Column 6 line 30 – Column 10 line 26). Trieger does not explicitly disclose a client computer is a cellular telephone (Column 13 lines 45 – 54). However, Owens discloses a method and/or system for validating subscribers which includes a wireless network, an authentication center which authenticates using the seed cryptographic key for first party by verifying the digital signature (Column 11 lines 2 – 48). Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of communication between first party and second party to exchange a seed value, a mathematical advance function

and one-way hash function as taught by Anderson and comparing security code with the generated security code to permit the respective communication to take place as taught by Trieger to provide wireless cellular telephone to authenticate the user as taught by Ownes. The motivation would have been to provide improved secure systems in cellular telephone.

Claim 22 is rejected as applied above in rejecting claim 21. Furthermore, Trieger teaches and describes a client computer connectable for secure communication with a server computer (Fig. 1 – 4 and Column 6 line 30 – Column 10 line 26). Trieger does not explicitly disclose that a client computer is a WAP enabled (Column 13 lines 44 – 54). However, Owens discloses a method and/or system for validating subscribers which includes a wireless network, an authentication center which authenticates using the seed cryptographic key for first party by verifying the digital signature (Column 11 lines 2 – 48).

Claim 23 is rejected under 35 U.S.C. 103(a) as being unpatentable over Trieger (U.S. Patent No.: 6,226,750) in view of Anderson (U.S. Patent No.: 5,751,812) further in view of Tang (U.S. Patent No.: 6,185,682).

Claim 23 is rejected as applied above in rejecting claim 18. Furthermore, Trieger teaches and describes a client computer connectable for secure communication with a server computer (Fig. 1 – 4 and Column 6 line 30 – Column 10 line 26). Trieger does

not explicitly disclose a client computer is a personal digital assistant (Column 13 lines 45 – 54). However, Tang discloses an authentication system wherein the client computer is a personal digital assistant (Column 4 lines 2 – 59). Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of communication between first party and second party to exchange a seed value, a mathematical advance function and one-way hash function as taught by Anderson and comparing security code with the generated security code to permit the respective communication to take place as taught by Trieger to have a personal digital assistant as client computer as taught by Tang. The motivation would have been to provide improved secure systems in Personal digital assistant.

Conclusion

6. Any response to this action should be mailed to:

Commissioner of Patents and Trademarks, Washington, D.C. 20231 **or faxed to:** (703) 872-9306 for all formal communications.

Hand-delivered responses should be brought to Crystal Park II, 2121 Crystal Drive, Arlington, VA, Fourth Floor (Receptionist).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Pramila Parthasarathy whose telephone number is 703-305-8912. The examiner can normally be reached on 8:00a.m. To 5:00p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Pramila Parthasarathy
Patent Examiner
703-305-8912
May 10, 2004

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100